www.igis.gov.au

Correspondence ref: 2014/855 File: 2014/41

Mr Dan Tehan MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House, Canberra

By email: pjcis@aph.gov.au

Dear Mr Tehan

Question on notice – retention of computer access warrant materials

At the Committee hearing on 15 August 2014 the Committee asked whether I though there should be a positive obligation that required ASIO to review the retention of information obtained under a warrant. The question was asked in the context of proposed changes to the definition of a 'computer' and a comment in my recent submission to the Committee that there was potential for a significant amount of information to be retained by ASIO about a person not relevant to security but who was the subject of, or created information on, a computer connected to a targeted network or system.

In my view it may be appropriate for the Committee to consider whether the legislation should create an obligation, such as that which exists in relation to police surveillance device warrants, to assess whether records are required to be retained after a period of time. This would have to be balanced against the resource implications for ASIO in making these decisions. My understanding of the comparable provisions relating to the retention of information collected under ASIO and law enforcement warrants is summarised in the attached table.

Yours sincerely

Vivienne Thom
Inspector-General
21 August 2014

PO Box 6181 K NGSTON ACT 2604
One National Circuit BARTON ACT 2600
Phone (02) 6271 5692 Fax (02) 6271 5696
E-mail info@igis.gov au

ASIO	**AFP**
Where ASIO has obtained information under an ASIO Act warrant (including a computer device warrant or a listening device warrant) there is no statutory obligation to review the need to retain that information. If the Director-General is satisfied that records, including copies of records, obtained under a warrant are not required for the performance of an ASIO function those records are to be destroyed: s31 ASIO Act	There is a positive obligation to destroy material within 5 years if the chief officer is not satisfied that a civil or criminal proceeding has been or is likely to be initiated or that the information is required some other specified purposes. This assessment needs to be made at least every 5 years. See s46 of the *Surveillance Devices Act 2004* (SD Act)
ASIO can communication information for purposes relevant to security (s18(1) & 18(2) of the ASIO Act); if the information is about a serious crime; is in the national interest; relates to a function of a Minister or Commonwealth or State official (s18(3)) and in other specified situations (see s18(4A), (4B) and s19(2)).	Police can disclose information obtained using a surveillance device for the purposes set out in s45 & 45(A) of the SD Act. These include the investigation and prosecution of certain crimes and also allow disclosure to ASIO
Section 64 & 65 of the *Telecommunications (Interceptions and Access) Act 1979* (TIA Act) allow ASIO to make use of and communicate intercepted material in connection with ASIOs functions.	Part 2-6 of the TIA Act sets out in some detail the purposes for which police can use intercepted information. Section 79 imposes an obligation to destroy 'restricted records' (a term which includes original records but not copies) if the chief officer is satisfied they are not likely to be required for a 'permitted purpose'.
Not subject to the Privacy Act but are to comply with Guidelines issued by the Attorney-General. Those Guidelines were amended in 2007 to, among other things, remove a prohibition on speculative data matching and make clear that ASIO was permitted to retain a comprehensive set of materials. Clause 6 of the Guidelines provides that ASIO may: (a) collect, maintain, analyse and assess information related to inquiries and investigations; (b) collect and maintain a comprehensive body of reference material… (c) maintain a broad database, based on the above… The Guidelines also require that ASIO only collect, use, handle or disclose personal information where reasonably necessary for the performance of its functions (cl 10)	Subject to the Privacy Act general rules on the collection, use and retention of personal information.

This is only a summary of the provisions. The provisions are quite detailed and the actual provisions should be referred to.